ABSTRACT OF THE DISCLOSURE

Apparatus and method of verifying personal identity of an authorized user and providing information necessary to gain access to one or more secure sites in response to such verification. The apparatus is embodied in a hand-held device having an input pad for a biometric parameter such as a finger (thumb) print, an LCD and a small keypad. The device is initialized by placing the authorized user's thumb on the input pad and pressing an enter key to store a template commensurate with the thumb print. Thereafter, the device may be activated only by a match of a print presented to the input pad with the previously stored template. By operation of scroll keys on the device keypad, the user enters names of secure sites to which access is desired. A unique password is generated by a random number generator and assigned to each secure site named. The password is stored both in the device and in the computer of the secure site. After activation of the device, previously stored site names and passwords may be recalled and displayed on the device by operation of the keypad. The password is then communicated to the secure site computer via a separate PC. Biometric data is not transmitted or stored in a data file, but exists only in encypted form in the device.